STATEMENT OF

LIEUTENANT GENERAL DAVID P. FRIDOVICH

DIRECTOR, SOCOM CENTER FOR SPECIAL OPERATIONS

BEFORE

THE HOUSE ARMED SERVICES SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS, AND CAPABILITIES

11 MARCH 2009

TRACKING AND DISRUPTING TERRORIST FINANCIAL NETWORKS: A POTENTIAL MODEL FOR INTER-AGENCY SUCCESS

STATEMENT OF LIEUTENANT GENERAL DAVID P. FRIDOVICH, DIRECTOR, SOCOM CENTER FOR SPECIAL OPERATIONS

BEFORE THE HOUSE ARMED SERVICES SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS, AND CAPABILITIES, 11 MARCH 2009

Chairman Skelton, Chairman Smith, Ranking Members McHugh and Miller, and distinguished members of the House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities:

Thank you for the opportunity to speak today on tracking and disrupting terrorist financial networks as a potential model for Inter-Agency success. I am honored to follow Mr. Frothingham, and strongly concur with his comments. 'All a brother needs for successful Jihad is himself and money.' So states enemy propaganda. Ideology has its role, but the more we study our enemy, the more we learn what we have always known: money talks, and disrupting its flow, especially from outside the combat zones, is a salient part of counter-terrorism. From United States Special Operations Command's role as Department of Defense lead I would like to briefly describe our efforts to disrupt terrorist financial facilitation networks, and applaud the outstanding interagency cooperation which is a hallmark of this effort.

Counterthreat Finance activities include, but are not limited to countering: narcotics trafficking, proliferation activities, weapons of mass destruction funding, trafficking in persons, weapons trafficking, precursor chemical smuggling, petty and organized crime, in some cases, very well organized crime.

Indeed, our enemy shows an impressive moral flexibility, engaging in every conceivable method of acquiring funds from running legal businesses and collecting voluntary donations, across the spectrum to kidnap for ransom and murder for hire. This enemy also operates across the technological spectrum, moving money on the backs of plodding animals and couriers across centuries old smuggling routes, or transferring money in seconds via the very latest in cell phone and internet technologies, and they continually adapt to our strategies against them.

Career terrorist facilitators are worthy adversaries, not to be underestimated. This is key, because to us at SOCOM it means very simply that DoD, no matter how we may adjust and organize, by ourselves, will fail to eliminate these networks. Likewise, the intelligence community, while adept at tracking, finds itself unequipped to disrupt, and law enforcement, operating independently, find convictions frustratingly hard to achieve. The enemy's flexibility, and great adaptability, compels us to take a whole-of-government, or interagency, approach to this challenge, looking well beyond traditional models, financial markets, and money movement methods. Likewise, we must work not only within our own interagency, but with the coalition, other partner nations, and the private sector. In this way, we can employ all available information, from the highest classification and most clandestine sources, to the latest public breaking stories. All geared towards disrupting the network, knowing it will reform rendered more vulnerable to further disruption in the future.

Within DoD, we are driven to take this effort beyond the combat zones, because the enemy has organized beyond the combat zones. Any tracking of money flows in support of the insurgents and terrorists operating in Iraq and Afghanistan links almost immediately to transregional and global facilitation networks that pose very real threats to the United States and our interests. Addressing this as a global problem, we at Special Operations Command have operationalized Department direction to synchronize Counterthreat Finance as the DoD lead, as part and parcel of our mission to synchronize overall DoD war plans and planning efforts.

USSOCOM is uniquely suited to this mission as we are a hybrid command, combining requirements to prepare train and equip special operations forces, with the synchronization mission, yet unlike the geographic combatant commands, we own no battlespace and thus are compelled to achieve results only

by, with, and through our DoD and interagency partners. Thus collaboration becomes essential to our way of doing business. Indeed, we pursue the Counterthreat Finance mission via four general methods, all of which are highly collaborative.

First, semi-annually, in April and October, we convene a Threat Finance Working Group as part of our Global Synchronization Conference. This brings together roughly 100 Counterthreat Finance analysts, investigators, and case agents from all the Geographic Combatant Commands, Functional Commands like Strategic Command and Joint Forces Command, the Combat Support Agencies, the InterAgency, most notably Treasury, State, FBI, DEA, and DHS/ICE, our British, Australian and Canadian colleagues, and various representatives of the private sector. This has become the premier forum for US Government Threat Finance exchange. Exchange with the coalition, and the private sector has been especially informative as we learn how better to deal with the rapidly developing cutting edge financial technologies like internet and cellphone money transfers.

I have studied testimony on this subject presented in 2005, and can see that this Threat Finance working group has become what was then envisioned by bringing community together and operationalizing each agency's unique knowledge, skills and authorities to maximize impact on financial facilitators.

Second, we hold semi-monthly Secure VideoTeleConferences to help develop DoD policy, procedures, and discuss specific networks and targets. These forums continue and sustain the focused energy of the Geographic Combatant Command Threat Finance units, now operating as part of their regional counterterrorism missions. These teams vary in size from twelve people at SOCOM to two in some commands, and mostly reside within each command wherever they can best connect to the interagency. Personnel are selected for prior interagency, law enforcement, or intelligence experience as the endeavor is very intelligence-intensive. We support Iraq and Afghanistan community specific videoteleconferences as well.

Third, we engage in robust continuous analyst exchange across the depth and breadth of the intelligence community, DoD, and the InterAgency. Information sharing is key. More on some of the mechanics of this in a moment. We are posting Threat Finance analysts, very carefully selected threat finance analysts, at several of the Combatant Commands, and we are working hard within the DoD community to develop Threat Finance analyst training. This highlights a simple key to fostering interagency success, which is to add value to other's efforts.

Fourth, we focus our analytical capabilities long term on carefully selected transregional targets which pose a clear threat to the US and our interests, and which are known to move and rely upon significant financial flows. We then share our expertise on these target sets with any and all InterAgency members, most especially Treasury and law enforcement, looking to operationalize results on targets DoD cannot currently reach via kinetic means. Right now these target sets include Al Qaida's External Facilitation Network, by which we mean those gentlemen operating in places like Kuwait and Pakistan, Europe and Asia to move money for IEDs, suicide-bombers and the like into Iraq and Afghanistan. We are also working against Al Shabaab, Lebanese Hezbollah and certain Iranian elements as they continue to develop a global financial facilitation infrastructure to rival that of Hezbollah and sometimes linked thereto.

While some in DoD, not so many years ago, saw this effort as well outside our lane, we have since seen the positive results. For example DoD is working to duplicate, outside of Iraq, the remarkable success of the Iraq Threat Finance Cell in thiw work, with which I believe you are now familiar. Such cells rely on fused efforts, taking intelligence to operators, who in the future, will be mostly law enforcement agents making arrests, rather than soldiers making captures or kills. Due to these successes, we are now eagerly participating in the establishment of the Afghanistan Threat Finance Cell.

While others exist, four particular interagency tools are the most effective, and thus most important. First, intelligence collection, which is done by all, for all, although signals intelligence is clearly one of the long poles in this tent. You are familiar with hawalas, the informal money transfer networks which circumvent formal financial institutions and traditional tracking methods. Widely used in the Middle East, and difficult to infiltrate, they pose a formidable financial collection challenge. However, as we study them, we find

many hawaladars employ varied levels of operational security. Most hawaladars, it must be said, run legitimate businesses, and serve a useful function for unbanked populations, but they seldom hesitate to move criminal or terrorist money, along with the legitimate. While threat finance is not an intelligence function, it is certainly intelligence-driven, and collection, careful, meticulous and often time-consuming collection, is critical.

Second, designations are one of the Treasury's best tools in the fight against terrorist financing. A tool we support. I defer to them for specifics of their programs but my people strongly support Treasury; we have a Liaison officer at Treasury, as does CENTCOM, and Treasury co-leads our aforementioned Global Synchronization Conference. Treasury co-leads the Iraq Threat Finance Cell, and is equally engaged in the formation of the Afghan Threat Finance Cell. A valuable point is that where the community once viewed designations as a final action, or mission accomplished, we now view them far more as an important bullet in a longer term volley. Let me explain.

A third tool is what DoD calls Information Operations, public affairs to some, or marketing. As a community, every time Treasury designates a terrorist facilitator, bad charity or company, we must leverage that action with volumes advertising why this was done to the target audience. Such efforts can enhance the impacts of Treasury and UN designations. This requires that underlying intelligence about criminal activity be declassified, a continual struggle.

And fourth, law enforcement actions, whether U. S. or partner nation arrests. Increasingly, we see Treasury designations as potentially enhancing and leading to such arrests. There are some exceptions to this and not all share this view, but these four tools offer far more as an ensemble than as individual actors.

Two key points about interagency collaboration. First, it is personality driven. We may wish it otherwise, but like the founders of this country, we must acknowledge the limits of human nature within which we work. Differing missions and approaches occasionally divide rather than unite, inhibiting information sharing. Thus, we choose personnel for interagency engagement with care and if previously productive organizational relationships turn sour, we investigate, and when necessary, make adjustments.

Downrange interagency relationships work very well, at Joint InterAgency Task Force-South in Key West, and in Iraq and Afghanistan, where the immediacy of the problems concentrates focus, focus that helps overcome the usual barriers to interagency cooperation and helps individuals bypass any other concerns towards achieving higher aims. Replicating that sort of mission focus, with a common view of the threat, is one of our keys to interagency or whole-of-government action and it is something DoD can, through robust intelligence collection and analytical support, wellcontribute to. We, the whole-of-government, focus on a given network, exactly what we know and don't know, how to fill those gaps, and then, which agency can address each node and in what way for maximum impact.

Second, information sharing drives this train. Not all issues here are solved, particularly the Intelligence community's continued penchant to overclassify, but we have made progress. For example, there is tear-lining of course, also law enforcement does not typically deal in the Secret and Top Secret realm, but rather, they speak of Law Enforcement Sensitive information. Within the Intelligence Community we have learned to call this Originator Controlled, or ORCON, thus we can share it within the community, but always with deference back to the originators of the information. This protects ongoing law enforcement investigations and sources. Likewise, when the IC shares Secret intelligence with law enforcement, for their possible subsequent use in judicial proceedings, law enforcement agents employ techniques of their own to render intelligence into usable evidence, while protecting sources. DEA and DoD from their years together in the drug war, are particularly good at these techniques.

The vital nature of information sharing goes beyond the US Government to include coalition and partner nations where, in some cases, counter-terrorism is of less interest, countering narcotics trafficking, human trafficking, or even prosecuting tax evasion however, are of great interest. In support of our law enforcement counterparts, we aid partner nations in making such charges, primarily through the exchange of intelligence and analytical expertise.

Dismantling an entire network is difficult, but the interagency has interdicted a number of individual facilitators. We can speak more specifically of these under other circumstances. Success in this arena is by its nature, not always conspicuous. These are investigations, often akin to organized crime investigations, which the law enforcement community can tell you, take years, not months. Sustaining the Counterthreat Finance effort is thus vital; likewise, if we are not to broaden our own authorities to take on facilitators wherever they may go, then we must work increasingly by, with and through our partner nations. This means the continued reinforcing of bilateral and multilateral relationships, aiding and training foreign governments in new ways to identify and report financial information, and to attack such networks.

I look forward to your questions.